UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/646,285	08/21/2003	Brett J. Willams	100205006-1	9347

22879 7590 07/14/2008
HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
SINGH, SATWANT K	
ART UNIT	**PAPER NUMBER**
2625	

NOTIFICATION DATE	DELIVERY MODE
07/14/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

Office Action Summary	Application No.	Applicant(s)	
	10/646,285	WILLAMS ET AL.	
	Examiner	Art Unit	
	SATWANT K. SINGH	2625	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 September 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 August 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This office action is in response to the amendment filed on 25 September 2007.

Response to Arguments

2. Applicant's arguments with respect to claims 1-31 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, 6-14, 15, 20-26, and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lamming et al. (US 6,922,725) in view of Cocotis et al. (US 2003/0078965).

5. Regarding Claim 1, Lamming et al teaches a method for providing a visitor safe wireless printer access point, the method comprising: connecting a wireless computing device to a wireless network, where the wireless network provides a public access point to a print spooling device (Fig. 3, S306) (computing device transmits a service discovery request over the first wireless communications channel) (col. 8, lines 44-59); determining all available printers in a secure wired network (multiple output devices may respond to the service discovery request) (col. 60-67); selecting one of available printers for printing (identify at least one output device) (col. 9, lines 1-12).

Lamming et al fails to teach a method for providing a visitor safe wireless printer access point, the method comprising: wherein the wireless computing device is permitted to access the available printer in the secure wired network and is prevented from accessing a secure device in the secure wired network; establishing a print path through the spooling device to the selected printer; sending a print job via the wireless network to the spooling device; spooling the print job on the spooling device; and sending the print job via the secure wired network to a selected printer from the available printers.

Cocotis et al teaches a method for providing a visitor safe wireless printer access point, the method comprising: wherein the wireless computing device is permitted to access the available printer in the secure wired network (accessing a remote public devices) (page 10, paragraph [0201]) and is prevented from accessing a secure device in the secure wired network (user authentication required for accessing any supported access device) (page 10, paragraph 0196]) (*It is being interpreted by the examiner that if the user does not have access to the access device, they will be denied access, however, the user can still access a remote public device.*); establishing a print path through the spooling device (repository) to the selected printer (print services stores the rendered image to a shared spooling service (i.e. repository), and sends a reference of the image to the Message Center, the Message Center uses the reference to output the data to the destination) (page 6, paragraph [0127]); sending a print job via the wireless network to the spooling device (MC retrieves the document to be printed and sends the document along with a rendering request to the destined print service) (page 11,

paragraph [0206]); spooling the print job on the spooling device (print service renders an output image of the document an saves it in output repository) (page 11, paragraph [0206]); and sending the print job via the secure wired network to a selected printer from the available printers (RDC sends the output image to the destined output device) (page 11, paragraph [00206]).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Lamming with the teaching of Cocotis to allow a user to wirelessly submit a print job behind a firewall without compromising the system's security.

6. Regarding Claim 6, Lamming et al teaches a method, wherein the action of determining all available printers in a secure wired network comprises: starting a utility application in the wireless device (begin a service request), where the utility application comprises a browser that is directed to the spooling device (user of the mobile computing device navigates the web browser to a web page that provides a list of directory services for a selected document) (col. 18, lines 54-67, col. 18, lines 1-4).

7. Regarding Claim 7, Lamming et al teaches a method, wherein the action of determining all available printers in a secure wired network comprises: starting a utility application in the wireless device (begin a service request), where the utility application comprises a network printer application that is configured to discover the available printers through the spooling device (web browser communicates with a web server operating on the document server) (col. 18, lines 54-67, col. 18, lines 1-4).

8. Regarding Claim 8, Lamming et al teaches a method, further comprising: downloading a printer driver from the spooling device to the wireless device; and initiating the printer driver in the wireless device (driver is loaded if necessary) (col. 10, lines 56-65).

9. Regarding Claim 9, Lamming et al teaches a method, further comprising: relaying a print job status from the printer, via the secure wired network, to the spooling device; and relaying the print job status from the spooling device, via the wireless network, to the wireless device (device status) (col. 9, lines 43-49).

10. Regarding Claim 10, Lamming et al teaches a method, wherein the wireless network is a wireless PRINT network (forming the first network is an output device) (col. 6, lines 50-55).

11. Regarding Claim 11, Lamming et al teaches a method, wherein the wireless PRINT network is a public access point to at least one print spooling device (Fig. 3, document server 108).

12. Regarding Claim 12, Lamming et al teaches a method, wherein the spooling device is configured to act as a bridge to send print jobs from the wireless device to the selected printer (an application program executes at or under the direction of the document server to render the document located at 320) (col. 10, lines 66-67, col. 11, lines 1-5).

13. Regarding Claim 13, Lamming et al teaches a method, wherein the spooling device is configured to act as a firewall to prevent access to a secure device in the

secured wired network (document services request are authenticated at firewall 1224) (col. 17, lines 38-48).

14. Regarding Claim 14, Lamming et al teaches an apparatus for providing a visitor safe wireless printer access point, the apparatus comprising: means connecting a wireless computing device to a wireless network by use of a printer access point device (mobile computing device communicates using an LCC transceiver) (col. 7, lines 54-67); means for transmitting the packet to a spooling device (parameters of the document service request are packaged and transmitted to the document server) (col. 10, lines 33-44), if the packet is an allowed packet (document service requests are authenticated) (col. 17, lines 38-48); means for downloading a printer driver and a printer driver information to the wireless computing device, and initializing the printer driver (driver is loaded if necessary for the specified output device that adapted to process the format in which the retrieved document exists) (col. 10, lines 55-65); and means for using the wireless computing device to print via an available printer in the secure wired network (output device outputs the rendered document) (col. 12, lines 51-61).

Lamming et al fails to teach if the wireless computing device is permitted to access the available printer in the secure wired network, and to prevent the wireless computing device from accessing a secure device in the secure wired network.

Cocotis et al teaches if the wireless computing device is permitted to access the available printer in the secure wired network (accessing a remote public devices) (page 10, paragraph [0201]), and to prevent the wireless computing device from accessing a

secure device in the secure wired network (user authentication required for accessing any supported access device) (page 10, paragraph 0196]) (*It is being interpreted by the examiner that if the user does not have access to the access device, they will be denied access, however, the user can still access a remote public device.*)

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Lamming with the teaching of Cocotis to allow a user to wirelessly submit a print job behind a firewall without compromising the system's security.

15. Regarding Claim 15, Lamming et al teaches an apparatus for permitting print operations from a network printer in a secure wired network, the apparatus comprising: a wireless computing device configured to connect to a wireless network, the wireless network including a public access point (Fig. 3, S306) (computing device transmits a service discovery request over the first wireless communications channel) (col. 8, lines 44-59).

Lamming et al fails to teach an apparatus for permitting print operations from a network printer in a secure wired network, the apparatus comprising: a print spooling device that is accessed from the public access point; wherein a print job is sent from the wireless computing device via the wireless network to the spooling device; wherein the wireless computing device is permitted to access at least one available printer in a secure wired network and is prevented from accessing a secure device in the secure wired network; and wherein the print job is spooled on the spooling device and the print

job is sent via a secure wired network to a selected printer that is selected from the at least one available printer.

Cocotis et al teaches an apparatus for permitting print operations from a network printer in a secure wired network, the apparatus comprising: a print spooling device that is accessed from the public access point (print services stores the rendered image to a shared spooling service (i.e. repository), and sends a reference of the image to the Message Center, the Message Center uses the reference to output the data to the destination) (page 6, paragraph [0127]); wherein a print job is sent from the wireless computing device via the wireless network to the spooling device (MC retrieves the document to be printed and sends the document along with a rendering request to the destined print service) (page 11, paragraph [0206]); and wherein the print job is spooled on the spooling device (print service renders an output image of the document an saves it in output repository) (page 11, paragraph [0206]); wherein the wireless computing device is permitted to access at least one available printer in a secure wired network (accessing a remote public devices) (page 10, paragraph [0201]) and is prevented from accessing a secure device in the secure wired network (user authentication required for accessing any supported access device) (page 10, paragraph 0196]) (*It is being interpreted by the examiner that if the user does not have access to the access device, they will be denied access, however, the user can still access a remote public device.*); and the print job is sent via a secure wired network to a selected printer that is selected from the at least one available printer (RDC sends the output image to the destined output device) (page 11, paragraph [00206]).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Lamming with the teaching of Cocotis to allow a user to wirelessly submit a print job behind a firewall without compromising the system's security.

16. Regarding Claim 20, Lamming et al teaches an apparatus, wherein the mobile wireless device is configured to start a utility application (begin a service request), where the utility application comprises a browser that is directed to the spooling device (user of the mobile computing device navigates the web browser to a web page that provides a list of directory services for a selected document) (col. 18, lines 54-67, col. 18, lines 1-4).

17. Regarding Claim 21, Lamming et al teaches an apparatus, wherein the mobile wireless device is configured to start a utility application (begin a service request), where the utility application comprises a network printer application that is configured to discover the available printers through the spooling device (web browser communicates with a web server operating on the document server) (col. 18, lines 54-67, col. 18, lines 1-4).

18. Regarding Claim 22, Lamming et al teaches an apparatus, wherein the spooling device is configured to download a printer driver to the wireless device, and wherein the printer driver is initiated in the wireless device (driver is loaded if necessary) (col. 10, lines 56-65).

19. Regarding Claim 23, Lamming et al teaches an apparatus, wherein a status of the print job is relayed from the printer, via the secure wired network, to the spooling

device; and wherein the status of the print job is also relayed from the spooling device, via the wireless network, to the wireless device (device status) (col. 9, lines 43-49).

20. Regarding 24, Lamming et al teaches an apparatus, wherein the wireless network is a wireless PRINT network (forming the first network is an output device) (col. 6, lines 50-55).

21. Regarding 25, Lamming et al teaches an apparatus, wherein the spooling device is configured to act as a bridge to send print jobs from the wireless device to the selected printer (an application program executes at or under the direction of the document server to render the document located at 320) (col. 10, lines 66-67, col. 11, lines 1-5).

22. Regarding 26, Lamming et al teaches an apparatus, wherein the spooling device is configured to act as a firewall to prevent access to a secure device in the secured wired network (document services request are authenticated at firewall 1224) (col. 17, lines 38-48).

23. Regarding Claim 31, Lamming et al teaches an article of manufacture, comprising: a computer-readable medium having stored thereon instructions to: connect a wireless computing device to a wireless network where the wireless network provides a public access point to a print spooling device (Fig. 3, S306) (computing device transmits a service discovery request over the first wireless communications channel) (col. 8, lines 44-59); determine all available printers in a secure wired network (multiple output devices may respond to the service discovery request) (col. 60-67); select one of available printers for printing (identify at least one output device) (col. 9, lines 1-12) .

Lamming et al fails to teach an article of manufacture, comprising: a computer-readable medium having stored thereon instructions to: wherein the wireless computing device is permitted to access the available printers in the secure wired network and is prevented from accessing a secure device in the secure wired network; establish a print path through the spooling device to the selected printer; send a print job via the wireless network to the spooling device, where the print job is spooled in a spooling device and sent via the secured wired network to a selected printer from the available printers.

Cocotis et al teaches an article of manufacture, comprising: a computer-readable medium having stored thereon instructions to: wherein the wireless computing device is permitted to access the available printers in the secure wired network (accessing a remote public devices) (page 10, paragraph [0201]) and is prevented from accessing a secure device in the secure wired network (user authentication required for accessing any supported access device) (page 10, paragraph 0196]) (*It is being interpreted by the examiner that if the user does not have access to the access device, they will be denied access, however, the user can still access a remote public device.*); establish a print path through the spooling device to the selected printer (print services stores the rendered image to a shared spooling service (i.e. repository), and sends a reference of the image to the Message Center, the Message Center uses the reference to output the data to the destination) (page 6, paragraph [0127]); send a print job via the wireless network to the spooling device (MC retrieves the document to be printed and sends the document along with a rendering request to the destined print service) (page 11, paragraph [0206]), where the print job is spooled in a spooling device (print service

renders an output image of the document an saves it in output repository) (page 11, paragraph [0206]) and sent via the secured wired network to a selected printer from the available printers (RDC sends the output image to the destined output device) (page 11, paragraph [00206]).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Lamming with the teaching of Cocotis to allow a user to wirelessly submit a print job behind a firewall without compromising the system's security.

24. Claim 27-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lamming et al. (US 6,922,725) in view of Cocotis et al. (US 2004/0190042) and Fong (US 2005/0243777).

25. Regarding Claim 27, Lamming et al teaches an apparatus for providing a visitor safe wireless printer access point, the apparatus comprising: a wireless computing device configured to connect to a wireless network with a printer access point device (Fig. 3, S306) (computing device transmits a service discovery request over the first wireless communications channel) (col. 8, lines 44-59).

Lamming et al fails to teach an apparatus for providing a visitor safe wireless printer access point, the apparatus comprising: a spooling device configured to download a printer driver and a printer driver information to the wireless computing device; and wherein the spooling device is configured to check a packet from the wireless computing device in order to determine if the wireless computing device is attempting to connect to an available printer in a secure wired network, and to transmit

the packet to the spooling device if the packet is an allowed packet, so that the wireless computing device can be used to print via the available printer in the secure wired network if the wireless computing device is permitted to access the available printer in the secure wired network, and wherein the wireless computing device is prevented from accessing a secure device in the secure wired network..

Cocotis et al teaches an apparatus for providing a visitor safe wireless printer access point, the apparatus comprising: a spooling device configured to download a printer driver and a printer driver information to the wireless computing device (remote device installation using centralized driver store) (page 5, paragraph [0104]) and if the wireless computing device is permitted to access the available printer in the secure wired network (accessing a remote public devices) (page 10, paragraph [0201]), and wherein the wireless computing device is prevented from accessing a secure device in the secure wired network (user authentication required for accessing any supported access device) (page 10, paragraph 0196]) (*It is being interpreted by the examiner that if the user does not have access to the access device, they will be denied access, however, the user can still access a remote public device.*)

Fong teaches an apparatus for providing a visitor safe wireless printer access point, the apparatus comprising: and wherein the spooling device is configured to check a packet from the wireless computing device in order to determine if the wireless computing device is attempting to connect to an available printer in a secure wired network, and to transmit the packet to the spooling device if the packet is an allowed packet, so that the wireless computing device can be used to print via the available

printer in the secure wired network (main server permits access only to those terminals that are registered) (page 6, paragraphs [0066] and [0067]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Lamming with the teachings of Cocotis and Fong to provide secure transmission of print jobs over a firewall without compromising the system's security.

26. Regarding Claim 28, Lamming et al teaches an apparatus, wherein the printer access point device is configured to check standard wireless security settings (request authenticated using the certificate server) (col. 17, lines 38-49).

27. Regarding Claim 29, Lamming et al teaches an apparatus, wherein the spooler device is configured to launch a print web page that shows at least one available printer in the secure wired network, in response to receipt of an allowed packet (Fig. 17, S1702-1712).

28. Regarding Claim 30, Lamming et al teaches an apparatus, wherein the printer access point device prevents the mobile wireless device from accessing a secured device in the secured wired network, if the wireless security settings are not correct (request authenticated using the certificate server) (col. 17, lines 38-49).

29. Claims 2-5, and 16-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lamming et al and Cocotis et al as applied to claim 1 and 15 above, and further in view of Fong (US 2005/0243777).

30. Regarding Claim 2, Lamming et al and Cocotis et al fail to teach a method, wherein the print job is split into network packets and transmitted to the spooling device, if the packets are allowed packets.

Fong teaches a method, wherein the print job is split into network packets and transmitted to the spooling device (mobile terminal sends data packets to the main server), if the packets are allowed packets (main server permits access only to those terminal that are registered) (page 6, paragraphs [0066]).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Lamming and Fong to prevent unauthorized access to the printing network to preserve system security.

31. Regarding Claim 3, Lamming et al and Cocotis et al fail to teach a method, wherein the packets are checked by the public access point device.

Fong teaches a method, wherein the packets are checked by the public access point device (main server receives the identification data packets from the server) (page 6, paragraphs [0067]).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Lamming and Fong to prevent unauthorized access to the printing network to preserve system security.

32. Regarding Claim 4, Lamming et al teaches a method, further comprising: in response to receipt of an allowed packet by the spooling device, launching a print web page that shows at least one available printer in the secure wired network (Fig. 17, S1712) (Fig. 17, S1704-1712) (col. 18, lines 53-67, col. 19, lines 1-4).

33. Regarding Claim 5, Lamming et al and Cocotis et al fail to teach a method, further comprising: if any one of the packets is not an allowed packet, then preventing the mobile wireless device from accessing a secure device in the secured wired network.

Fong teaches a method, further comprising: if any one of the packets is not an allowed packet, then preventing the mobile wireless device from accessing a secure device in the secured wired network (main server permits access only to those terminals that are registered) (page 6, paragraphs [0066]).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Lamming and Fong to prevent unauthorized access to the printing network to preserve system security.

34. Regarding Claim 16, Lamming et al and Cocotis et al fail to teach an apparatus, wherein the print job is split into network packets and transmitted to the spooling device, if the packets are allowed packets.

Fong teaches an apparatus, wherein the print job is split into network packets and transmitted to the spooling device (mobile terminal sends data packets to the main server), if the packets are allowed packets (main server permits access only to those terminal that are registered) (page 6, paragraphs [0066]).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Lamming and Fong to prevent unauthorized access to the printing network to preserve system security.

35. Regarding Claim 17, Lamming et al and Cocotis et al fail to teach an apparatus, wherein the packets are checked by the public access point device.

Fong teaches an apparatus, wherein the packets are checked by the public access point device (main server receives the identification data packets from the server) (page 6, paragraphs [0067]).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Lamming and Fong to prevent unauthorized access to the printing network to preserve system security.

36. Regarding Claim 18, Lamming et al teach an apparatus, wherein the spooling device is configured to launch a print web page that shows at least one available printer in the secure wired network, in response to receipt of an allowed packet by the spooling device (Fig. 17, S1704-1712) (col. 18, lines 53-67, col. 19, lines 1-4).

37. Regarding Claim 19, Lamming et al and Cocotis et al fail to teach an apparatus, wherein the mobile wireless device is prevented from accessing a secure device in the secured wired network, if any one of the packets is not an allowed packet.

Fong teaches an apparatus, wherein the mobile wireless device is prevented from accessing a secure device in the secured wired network, if any one of the packets is not an allowed packet network (main server permits access only to those terminals that are registered) (page 6, paragraphs [0066]).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Lamming and Fong to prevent unauthorized access to the printing network to preserve system security.

Conclusion

38. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SATWANT K. SINGH whose telephone number is (571)272-7468. The examiner can normally be reached on Monday thru Friday 8am - 4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David K. Moore can be reached on (571) 272-7437. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Satwant K. Singh
Examiner
Art Unit 2625

sks

/Twyler L. Haskins/
Supervisory Patent Examiner, Art Unit 2625